

Trusted Digital Repositories

A systems approach to
determining trustworthiness
using DRAMBORA



DRAMBORA

Digital Repository Audit Method Based on Risk Assessment

A self-audit toolkit developed by the
Digital Curation Centre (DCC)

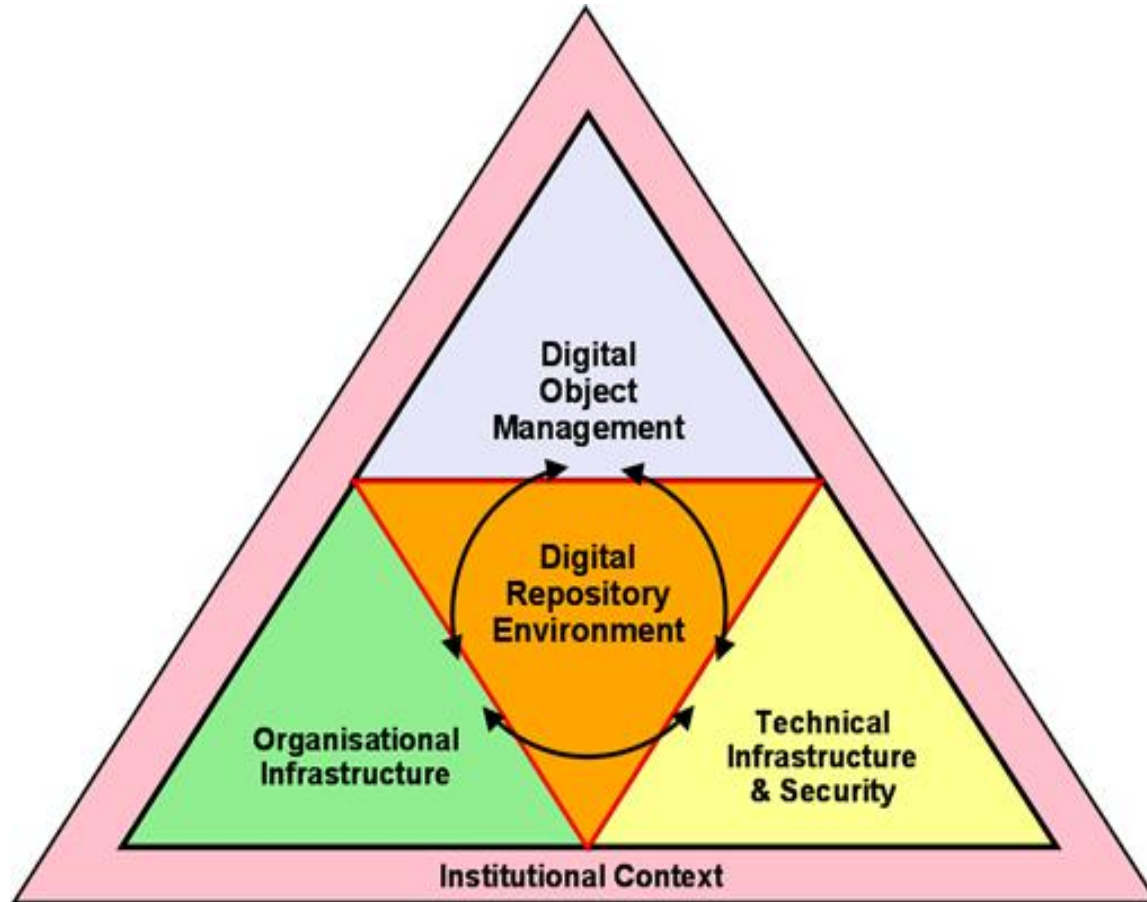
<http://www.dcc.ac.uk/FAQs/self-auditing/>



DSPACE

DRAMBORA

The 3 legs of a TDR



LEG 1:

Organizational Infrastructure



organization = system

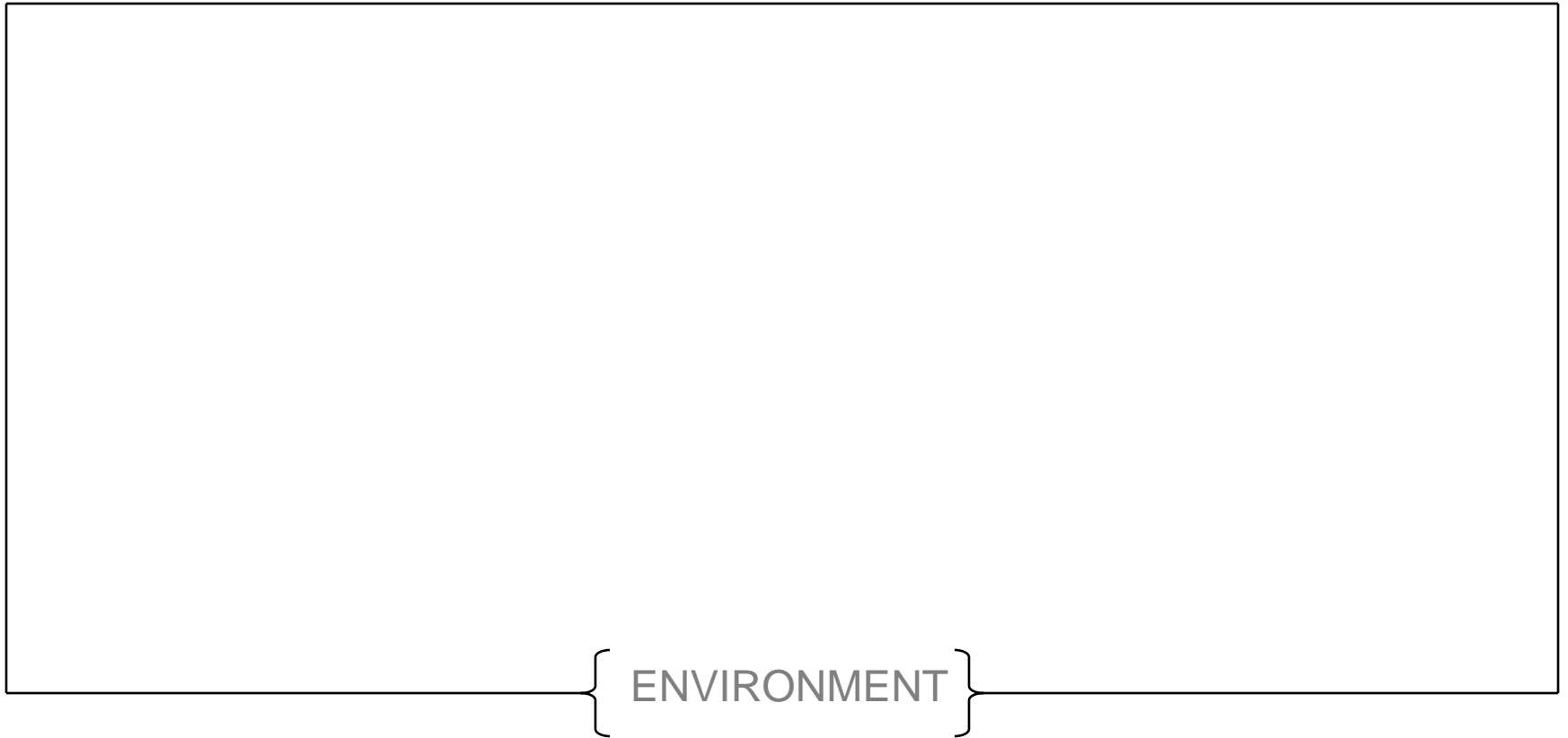


what is a system?

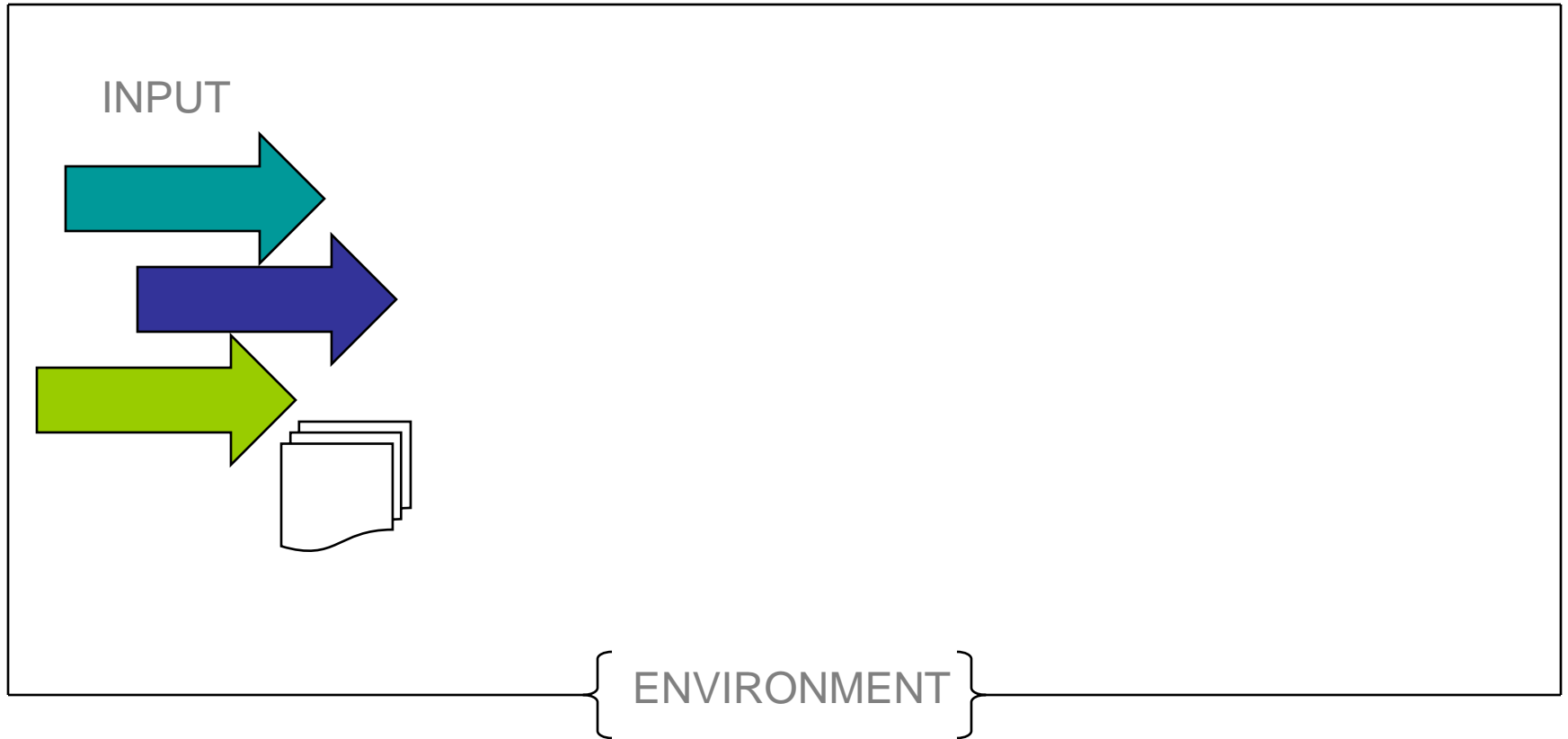


DSPACE

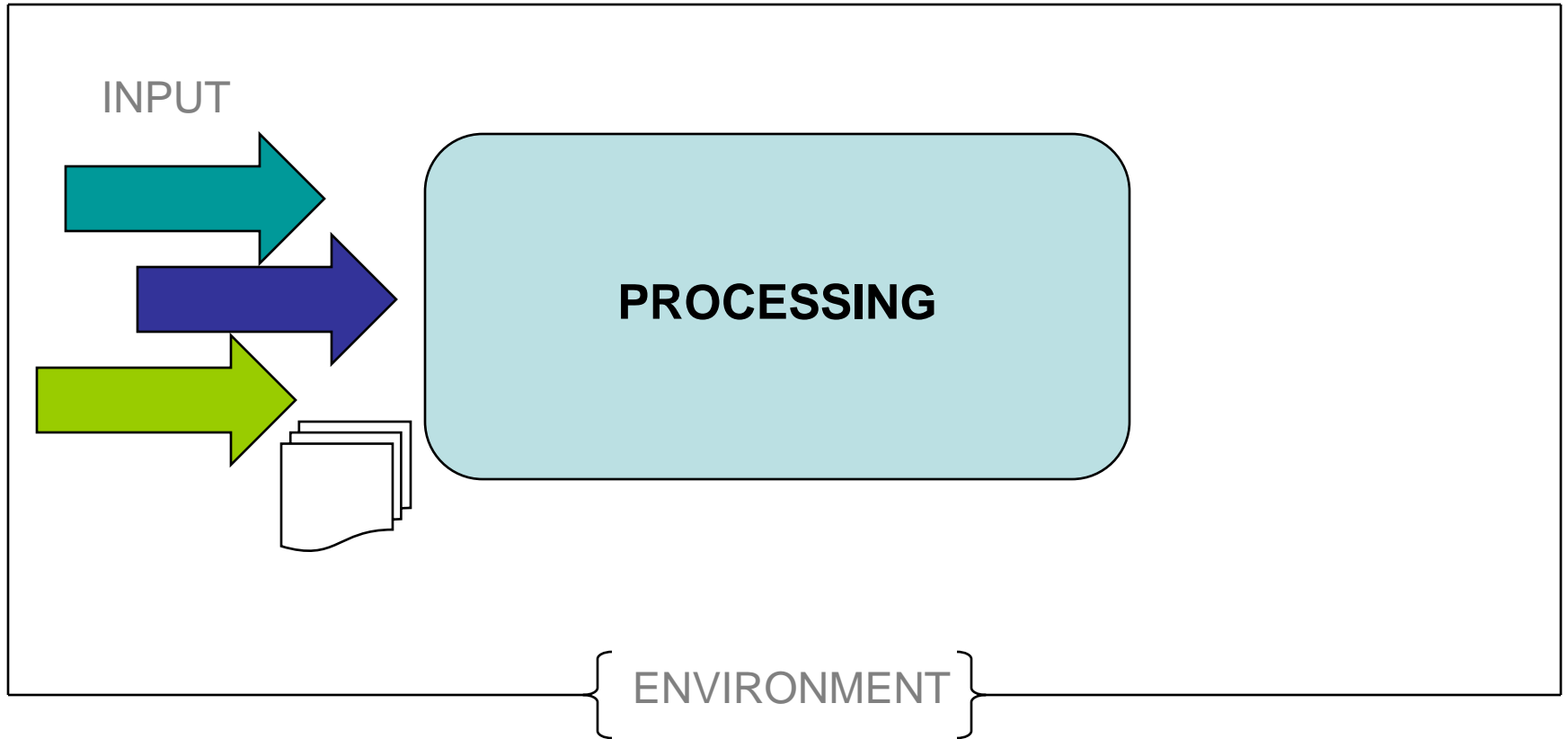
System: generic



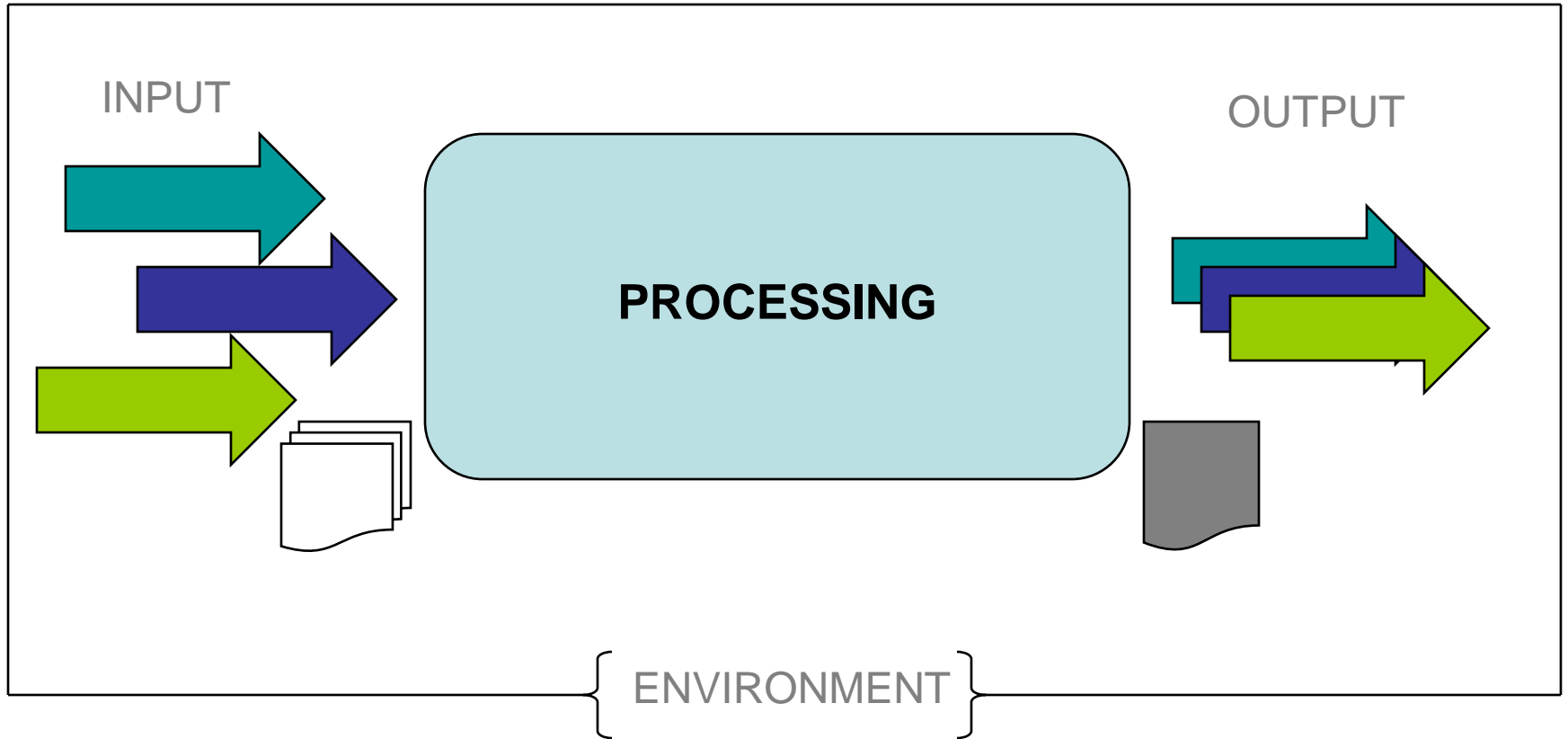
System: generic



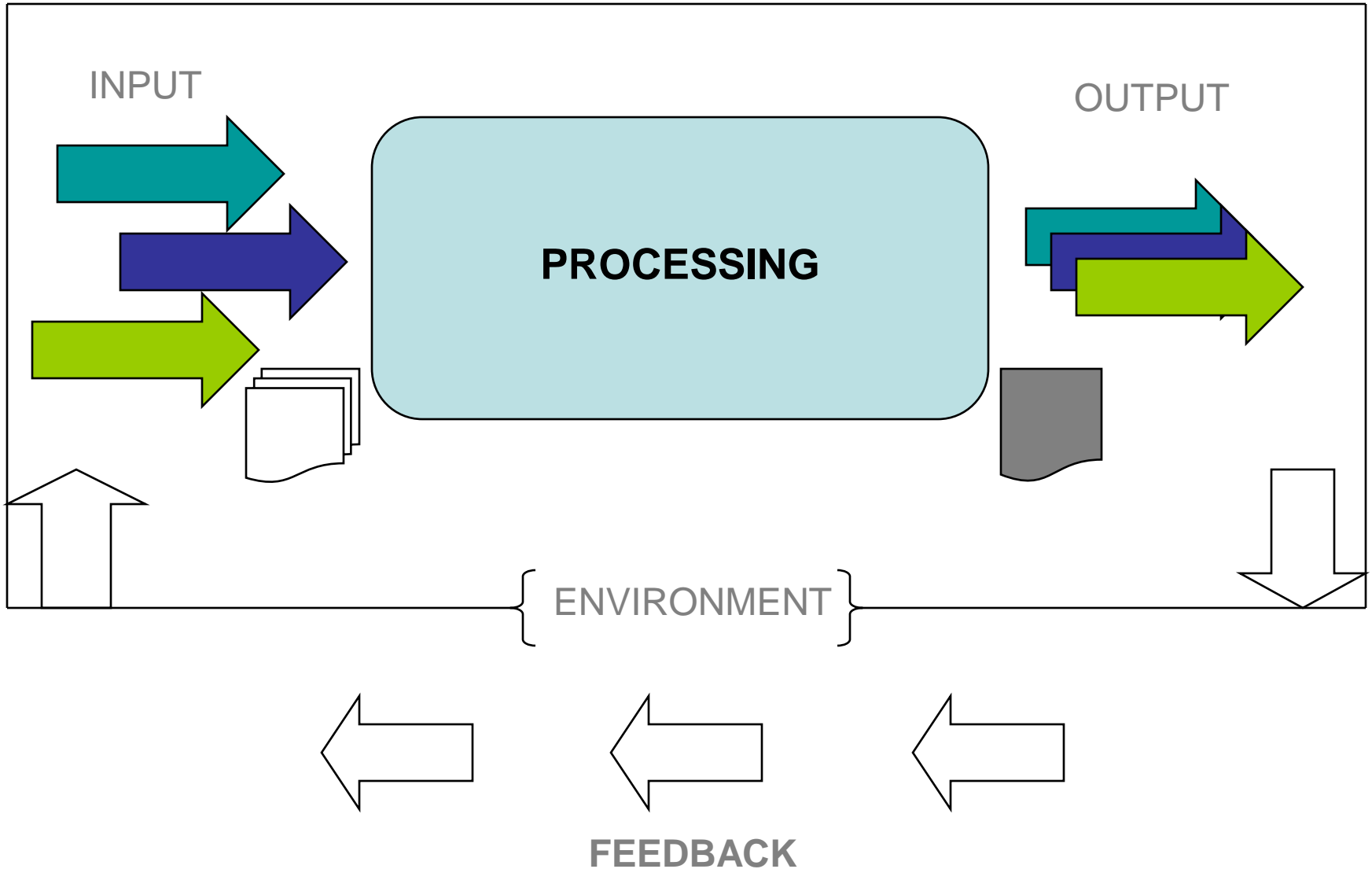
System: generic



System: generic

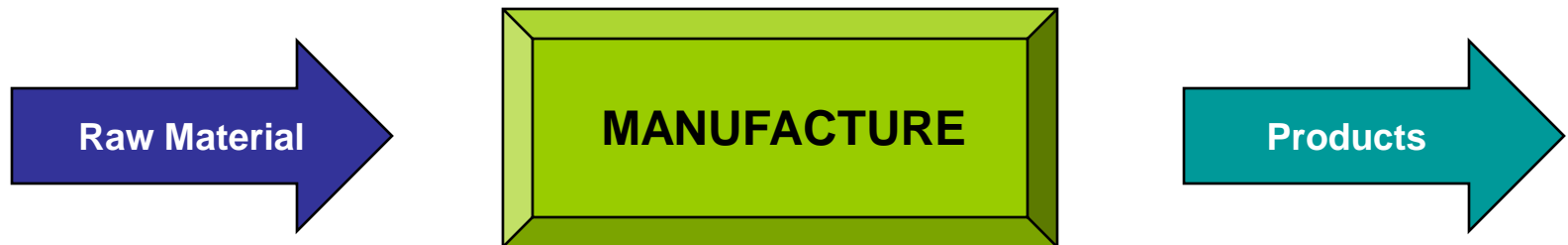


System: generic



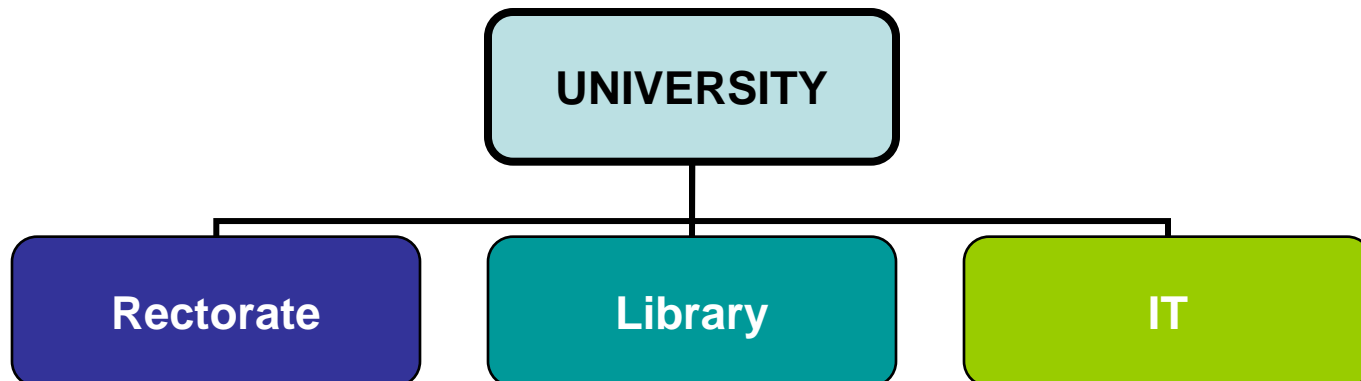
System: organization

- Any organization is a system
- A system of people, finances, assets, intellectual property, products
- Product management is a system:



System: IR

- Generally called an **Institutional** repository
 - Institutional = Organizational
 - Organization = System
 - University = Organization = System
 - Systems within a system
 - Libraries within Universities
 - Library is one system within the larger (network of) systems
- ✓ Libraries aren't solely responsible for a [...] Repository



System: **trusted** IR

Question: what is a **trusted** [...] repository?

Answer: you heard Ina {quote}:

“

...

capable of providing reliable, long-term access
to managed digital resources, to a designated
community

”

...

(RLG-OCLC Report 2002)

System: **trusted** IR

Question: what is a **trusted** [...] repository?

Answer: you heard Ina {quote}:

“...a network of *systems*, *roles* and *responsibilities* capable of providing reliable, long-term access to managed digital resources, to a designated community
...”

(RLG-OCLC Report 2002)

System: **trusted** IR

{ “A digital repository is a complex and interrelated system. In determining trustworthiness, one must look at the **entire** system in which the digital information is managed, including the **organization** running the repository: its governance; **organizational** structure and staffing; policies and procedures; financial fitness and sustainability; the contracts, licenses, and liabilities under which it must operate; and **trusted** inheritors of data, as applicable.” }

(RLG-OCLC Report 2002)

System: **trusted** IR

{ “A digital repository is a complex and interrelated system. In determining trustworthiness, one must look at the **entire** system in which the digital information is managed, including the **organization** running the repository: **its governance**; **organizational** structure and staffing; **policies and procedures**; **financial fitness and sustainability**; the contracts, licenses, and liabilities under which it must operate; and **trusted** inheritors of data, as applicable.” }

(RLG-OCLC Report 2002)

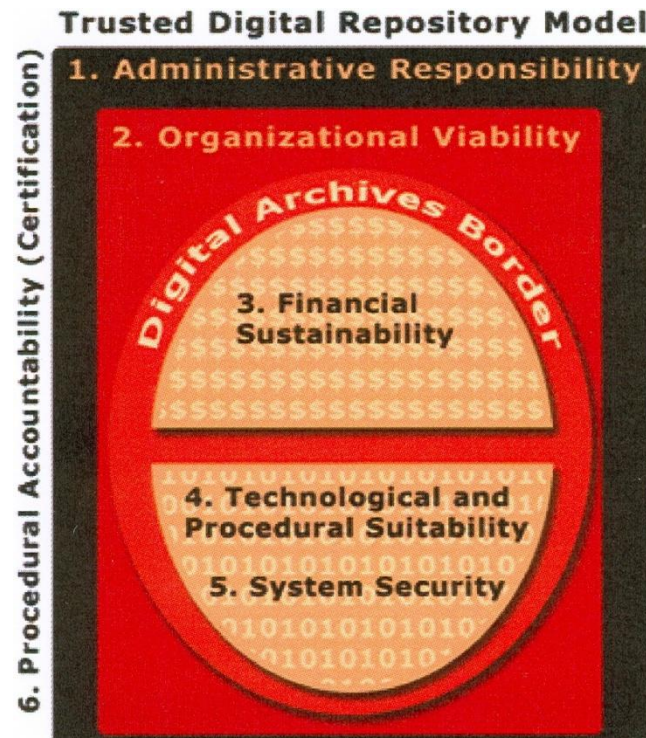
Attributes: Trusted IR

The RLG-OCLC report recognizes 6 attributes of a Trusted Digital Repository:

Attribute	Description
Administrative responsibility	Meet national/international standards, provide evidence of commitment to implementing standards and best practices.
Organizational viability	Reflect commitment to long-term retention/management in mission statements, undertake risk management, contingency and succession planning, demonstrate viability and trustworthiness.
Financial sustainability	Demonstrate financial fitness and ongoing financial commitment, establish and maintain good business practices and an auditable business plan.
Technological suitability	Consider and adopt appropriate preservation strategies, ensure appropriate infrastructure (hardware, software, facilities) for storage and access, establish technology management policy for repository.
System security	Assure security of digital assets, establish procedures to meet requirements (copying, authentication, firewalls, backups, disaster recovery).
Procedural accountability	Enact all relevant policies and procedures for specified tasks and functions, document all practices.

Attributes: **Trusted IR**

The attributes with a *Digital Archives Border* to group one or more repositories within an organization or consortium.



A model of a trusted digital repository developed by Nancy Y. McGovern with Anne R. Kenney for the Digital Preservation Management workshop series, 2003, based on an analysis of the attributes of a trusted digital repository. The digital archives border was added by the designers of the model.

LEG 2:

Technical Infrastructure and System Security



Attribute 4: System Infrastructure

See Section C.1 of TRAC (Trustworthy Repositories Audit & Certification: Criteria and Checklist)

Specifies:

1. function on a well supported Operating System (e.g. Ubuntu **L**ong **T**erm **S**upport)
2. adequate hardware and software support for backup functionality sufficient for the IR
3. mechanisms in place to ensure multiple copies are synchronized
4. has a process to react to the availability of new software security updates – that's why we are *learning* to install and patch DSpace
5. etc.

Attribute 5: System Security

See Section C.3 of TRAC (Trustworthy Repositories Audit & Certification: Criteria and Checklist)

Amongst others refers to servers, firewalls, routers, fire protection and flood detection systems and all other IT processes related to system security which will demonstrate that the digital repository has suitable disaster recovery plan(s) appropriate to the repository's location and service expectations.

Systems approach

Various things must be done:

1. Sign SLA's.
2. Install digital repository software on institutional infrastructure
3. Go virtual
4. Separate the database back-end
5. Off-site storage of backups
6. Replicate your data store
7. Expand the OAIS model to suit your organizational needs
8. Etc.

LEG 3:

Digital Object Management

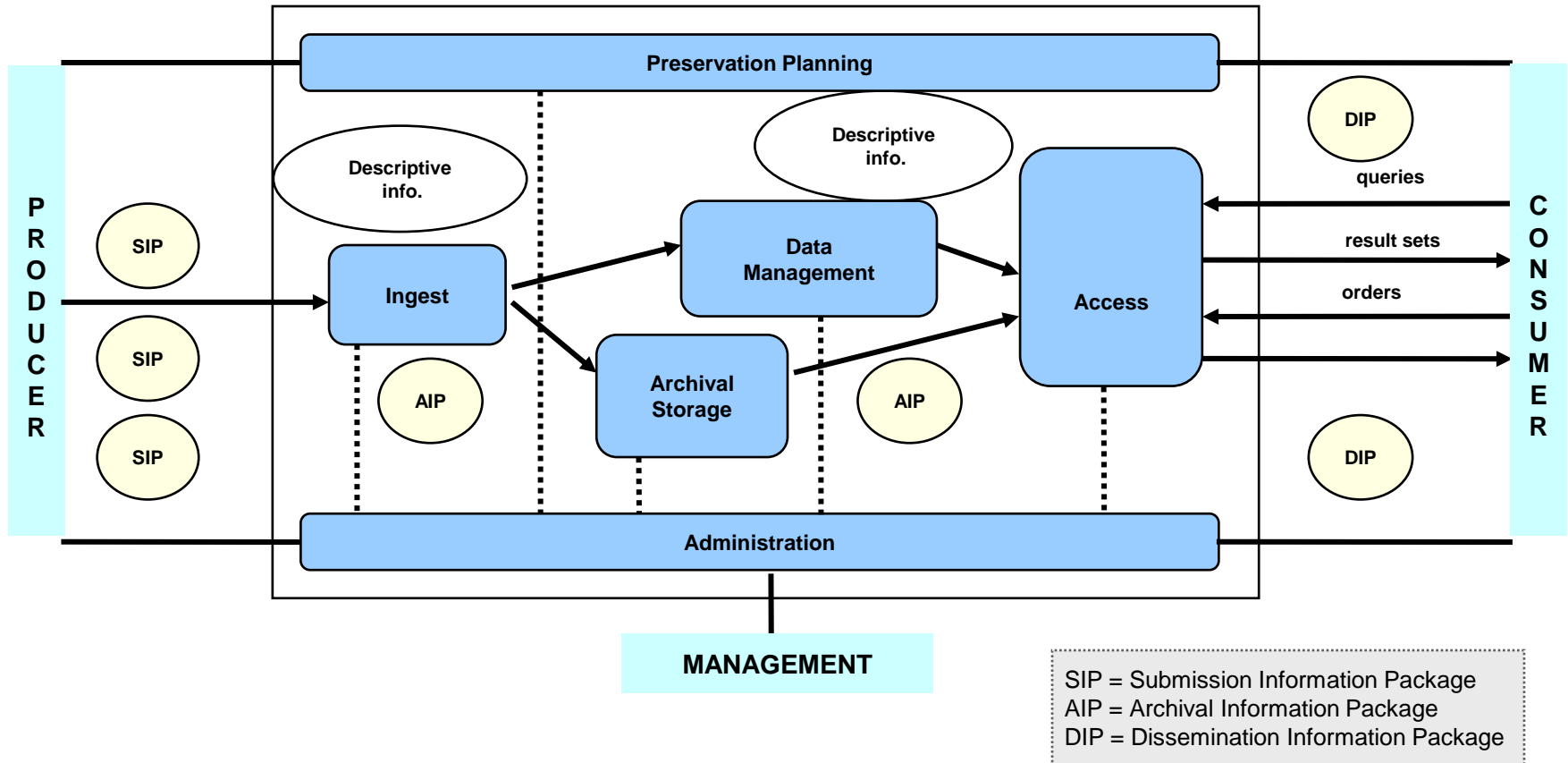


System: OAIS

- **Open Archival Information System**
- Ratified standard = ISO14721:2003
- *A reference model* for a functional system
- Describes in no prescriptive terms an **organization** of (1) people and (2) systems
- Illustrates there are systems within a system
- Contains:
 1. roles (the people)
 2. entities (the software)
 3. functions (the workflows)



OAIS overview



Conclusion

- DSpace = digital repository software
- DSpace on a server does not in itself determine trustworthiness
- OAIS in itself does not determine trustworthiness
- A *systems* approach COULD determine trustworthiness
- System = Organization
- Involve your organization!

